UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,570	03/10/2005	Markus Bockes	WACHP006	7328

25920 7590 10/13/2010

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/13/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,570	BOCKES ET AL.	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 August 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,14-20,22-32 and 34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,14-20,22-32 and 34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 14-20, 22-32, and 34 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/17/2010 has been entered.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1, 14-20, 22-32, and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Seifert et al. USPN 7248700 B2.**

Regarding claims 1 and 30, Seifert et al teaches a method/product for protected execution of a cryptographic calculation **[see col. 3 lines 48-67 and figs. 1-2B]**, in which a key with at least two key parameters is drawn on **[see col. 5 lines 61-67; p, q …; see also col. col. 4 lines 1-21]**, wherein the key is a private RSA key for use in an RSA method **[see col. 5 lines 61-col. 6 lines**

38], wherein each key parameter is a private RSA key parameter contained in the private RSA key **[see claim 1 and figs 1-2A]**, wherein an integrity check of the private RSA key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter **[see fig. 2B and see col. 7 lines 24-35]**, wherein the cryptographic calculation is one of a decryption in the RSA method and a signature generation in the RSA method **[see claim 2, and abstract]**, and wherein each operation of the method for protected execution of the cryptographic calculation is executed by an integrated circuit **[col. 7 lines 24-31 and col. 3 lines 48-67 and figs. 1-2B]**.

Regarding claim 27 Seifert et al. teaches a method for determining a key for a cryptographic calculation **[see col. 3 lines 48-67 and figs. 1-2B]** with at least two key parameters **[see col. 5 lines 61-67; p, q …; see also col. col. 4 lines 1-21]**, wherein the key is a private RSA key for use in an RSA method **[see col. 5 lines 61-col. 6 lines 38]**, and wherein each key parameter is a private RSA key parameter contained in the private RSA key **[see claim 1 and figs 1-2A]**, the key being adapted to be used in a method for protected execution of a cryptographic calculation wherein an integrity check of the private RSA key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter **[see fig. 2B and see col. 7 lines 24-35]**, wherein the cryptographic calculation is one of a decryption in the RSA method signature generation in the RSA method **[see claim 2, and abstract]**, and wherein each operation of the method for determining the private RSA key for the cryptographic calculation is executed

by an integrated circuit **[col. 7 lines 24-31 and col. 3 lines 48-67 and figs. 1-2B]**.

Regarding claim 32 Seifert et al. teaches a portable data carrier comprising a processor and a storage, the storage having a computer program stored thereon, the computer program including program commands to cause the processor to execute a method for protected execution of a cryptographic calculation **[see col. 3 lines 48-67 and figs. 1-2B]**, in which a key with at least two key parameters is drawn on **[see col. 5 lines 61-67; p, q …; see also col. col. 4 lines 1-21]**, wherein the key is a private RSA key for use in an RSA method **[see claim 1 and figs 1-2A]**, wherein each key parameter is a private RSA key parameter contained in the private RSA key **[see claim 1 and figs 1-2A]**, wherein an integrity check of the private RSA key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter **[see fig. 2B and see col. 7 lines 24-35]**, wherein the data carrier is one of a smart card and a chip module **[col. 7 lines 24-31 and col. 3 lines 48-67 and figs. 1-2B]**, and wherein the cryptographic calculation is one of a decryption in the RSA method and a signature generation in the RSA method **[see claim 2, and abstract]**.

Regarding claim 14 Seifert et al. teaches the method, wherein in the integrity check it is determined whether the value of at least one private RSA key parameter is contained in a range of valid values, wherein the range is non-contiguous in that it has a plurality of gaps **[see fig. 2B and see col. 7 lines 24-35]**.

Regarding claim 15 Seifert et al. teaches the method, wherein in the integrity check it is determined whether at least two private RSA key parameters are in a predetermined relationship to one another **[see col. 4 lines 1-63].**

Regarding claim 16 Seifert et al. teaches the method, wherein the integrity check includes a multiplicative operation, in particular a divisibility test **[see fig. 2B and see col. 7 lines 24-35]**.

Regarding claim 17 Seifert et al. teaches the method, wherein in the integrity check it is checked whether at least one of the private RSA key parameters is evenly divisible by a safeguard value **[col. 6 lines 1-58 and fig. 2a-2b]**.

Regarding claim 18 Seifert et al. teaches the method, wherein in the integrity check it is checked whether at least one value which differs from one of the private RSA key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value **[see claim 1 and figs. 1-2b]**.

Regarding claim 19 Seifert et al. teaches the method in the integrity check a checksum stored with the private RSA key parameters is compared with a checksum newly calculated after passing of the private RSA key parameters **[see fig. 2B and see col. 7 lines 24-35]**.

Regarding claim 20 Seifert et al. teaches the method wherein, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing **[see fig. 2B**

and see col. 7 lines 24-35].

Regarding claim 22 Seifert et al. teaches the method wherein the RSA method is an RSA-CRT method **[see abstract and col. 3 lines 64-67].**

Regarding claim 23 Seifert et al. teaches the method wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value **[see claim 1, fig. 2B and see col. 7 lines 24-35]**.

Regarding claim 24 Seifert et al. teaches the method wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying **[see col. 7 lines 24-35 and fig. 2b]**.

Regarding claim 25 Seifert et al. teaches the method wherein the prime factors of the RSA method are multiplied by a masking parameter and an error freedom of the calculation sequence is checked by an equality check modulo the masking parameter **[see col. 7 lines 24-35 and figs. 1-2b]**.

Regarding claim 26, 29, 31 and 34 Seifert et al. teaches the method/product/data carrier, wherein at least one private RSA key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check

[see fig. 2b and see col. 7 lines 24-35].

Regarding claim 28 Seifert et al. teaches the method wherein at least one private RSA key parameter is obtained by multiplication of a value required for the cryptographic calculation by a safeguard value **[see col. 4 lines 1-63 and figs. 1-2A].**

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 6:00am-2:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Primary Examiner, Art Unit 2436